Research proposal

Quantum Cryptography for Online Banking System

Guide:
Prof.(Dr.) S.K.Lenka

Scholar:
Anand Sharma

Faculty of Engineering and Technology
Mody Institute of Technology and Science, Lakshmangarh

1

Content

- Network Security
- Cryptography
- Quantum cryptography
- Quantum Key Distribution Protocol
- QKD Attributes
- Recent Status
- Research and Development Areas
- Application Areas
- Online Banking
- Proposed Research
- Expected Challenges
- Publications
- References

2

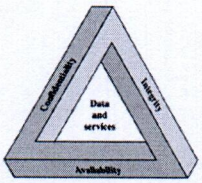
Network Security

Security Parameters

- Confidentiality
- Integrity
- Availability
- Authenticity
- Accountability

Security Services

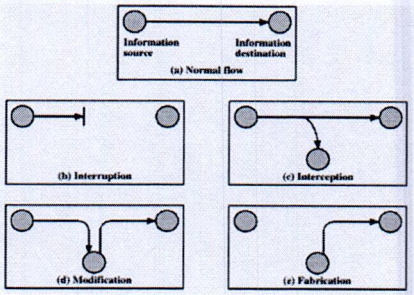
- Data Confidentiality
- Access Control
- Authentication
- Data Integrity
- Non-repudiation



CIA Triad

3

Security Threats



4

Cryptography

Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication.

Cryptanalysis is the study of mathematical techniques for attempting to defeat cryptographic techniques, and, more generally, information security services.

Plaintext	*M*
Encryption	*E(M) = C*
Ciphertext	*C*
Decryption	*D(C) = M*

Cryptography + Cryptanalysis = Cryptology

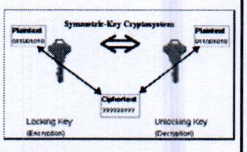
5

Types of Cryptography

Symmetric (Private-Key) Algorithms

$E_K(M) = C$
$D_K(C) = M$

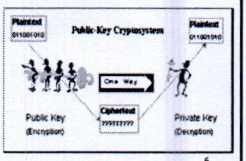
- *DH Key Exchange*
- DES
- Triple DES



Asymmetric (Public-Key) Algorithms

$E_{K1}(M) = C$
$D_{K2}(C) = M$

- *RSA Algorithm*
- Key Distribution
- Digital Signature



6

Limitations of Classical Cryptography

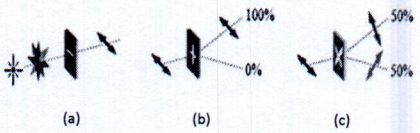
- Distribution of the key is the main problem with classical cryptography.
- Security relies on unproven mathematical assumptions such as difficulty of factoring integers.
- A quantum computer can easily crack all possible classical cryptographic solutions.
- Classical cryptographic is vulnerable to quantum attacks.

7

Quantum Cryptography

The Quantum Cryptography basically depends upon :

1. Heisenberg Uncertainty Principle
2. Principle of Photon Polarization.

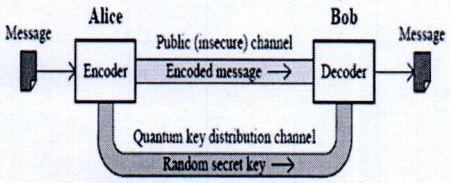


Qubit as a polarized photon.

8

Quantum Cryptography contd.....

Conventional Model for Quantum Cryptography



Quantum Cryptography

9

Quantum Key Distribution

Protocols :

- BB84 (Bennett, Charles H. and Brassard, Gilles) 1984
- E91 (Ekert, Artur K.) 1991
- B92 (Bennett, Charles H.) 1992

10

QKD : BB84

Bennett, Charles H.
IBM Research, USA

Brassard, Gilles
University of Montreal, Canada

11

QKD : BB84 contd.....

1. 0 0 1 1 1 0 0 0 1 1 1 0 0 0 1
   *Alice prepares random **values** for key bits.*
2. *Alice transmits each random value encoded in a random, non-orthogonal **basis** on a "single photon."*
3. *Bob randomly selects a basis and measures each photon.*
4. √ - √ √ √ - √ - - - - √ √ - √
   Alice and Bob publicly communicate to determine matching bases, and discard all other bits ("sifting").
5. 0 - 1 1 1 - 0 - - - - 0 0 - 1
   *Now Alice and Bob share matching **values** for key bits (assuming no errors!).*

12

QKD Attributes

- Confidentiality of Keys
- Sufficiently Rapid Key Delivery
- Authentication
- Robustness
- Error Correction
- Privacy Amplification

13

Recent Status

id Quantique (Geneva)
MagiQ Technologies (New York)
SmartQuantum (France)

DARPA :

Research Leader	Research Location	Research Focus
P. Grangier	Paris	Experiment
G. Leuchs	Erlangen	Experiment
E. Giacobino	Paris	Experiment
N. Cerf	Brussels	Theory
J. Preskill	Caltech	Theory

14

Research and Development

- Authentication for Quantum Message
- Quantum bit commitment
- Quantum data hiding
- Secure multiparty quantum computation
- Quantum-computational security

15

Applications

- Online Banking
- *E-Voting*
- *Wireless LAN*
- *Free-Space Optical QKD*
- *QKD Networks*
- Military Communication

16

Online Banking

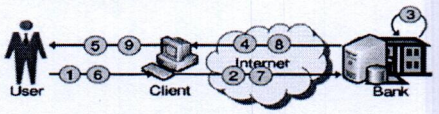
Online banking is the newest delivery channel for retail banking services. Online banking facilitated by various Electronic Commerce technologies.

The range of functions that are usually offered by telecommunication systems of online banking include displaying balances and statements, paying bills, transferring money between accounts, viewing standing orders and direct debits, viewing transactions with a search and sort facility.

17

Online Banking

contd.....



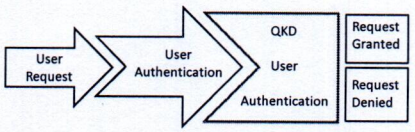
Authentication in online Banking

1. Produce Login Id and Pass-code
2. Transmit Login Id and Pass-code
3. Verify Login Id and Pass-code
4. Transmit service options
5. Present service options
6. Transaction request
7. Transmit transaction request
8. Transmit transaction confirmation
9. Present transaction confirmation

18

Proposed Research

Quantum Cryptography in Online Banking

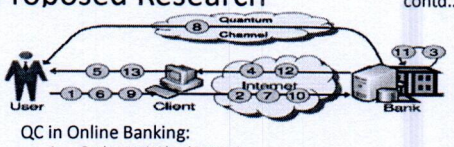


Model for Authentication through Quantum Cryptography in Online Banking

19

Proposed Research

contd.....



QC in Online Banking:

1. Produce Login Id and Pass-code
2. Transmit Login Id and Pass-code
3. Verify Login Id and Pass-code
4. Transmit service options
5. Present service options
6. Transaction request
7. Transmit transaction request
8. Quantum Key Distribution
9. Produce Quantum code
10. Transmit Quantum code
11. Verify Quantum code
12. Transmit transaction confirmation
13. Present transaction confirmation

20

Benefits of having QC

- Mathematically unbreakable, Security is based on laws of physics.
- It allows to detect any eavesdropping.
- Will still be secure even if Quantum Computer is built.

21

Expected Challenges

- Photon Sources
- Quantum Channels
- Single Photon Detection
- Quantum Repeaters

22

Publications

Papers summarizes the current state of quantum cryptography and provides potential extensions of its feasibility as a mechanism for securing existing communication systems.

1. Anand Sharma and S.K. Lenka "Quantum Cryptography for Online Banking" Communicated.
2. Anand Sharma, Vibha Ojha, and S.K.Lenka "Quantum Key Distribution in WLAN 802.11 Networks" in proceeding of *2010 IEEE International Conference on Networking and Information Technology (ICNIT 2010) Manila, Philippines*, pp. 402-405.
3. Anand Sharma, Vibha Ojha, and S.K.Lenka "Security of Entanglement Based Version of BB84 protocol for Quantum Cryptography" in proceeding of *3rd IEEE International Conference on Computer Science and Information Technology (IEEE ICCSIT 2010) Chengdu, China*, pp.615-619.

23

References

1. C.H. Bennet and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," Proc. Int'l Conf. Computers, Systems & Signal Processing, CS Press, 1984, pp. 175–179.
2. Artur Ekert, *"Quantum Cryptography based on Bell's Theorem"*, Physical Review Letters, 1991.
3. Bennett, Charles H., "Quantum cryptography using any two nonorthogonal states", Physical Review Letters, Vol. 68, No. 21, 25 May 1992, pp 3121 - 3124.
4. W. Tittel, G. Ribordy, and N. Gisin. "Quantum cryptography". Physics World, 11:41-45, (1998)
5. C. Elliott, D. Pearson, and G. Troxel, "Quantum Cryptography in Practice," Proc. ACM SIGCOMM 2003, ACM Press, 2003, pp. 227–238.
6. Einstein, A., B. Podolsky, N. Rosen, "Can quantum, mechanical description of physical reality be considered complete?", Phys. Rev. 47, 777 (1935)
7. C.S. Elizabeth Daniel, On-line Banking: Strategic and Management Challenges, Long Range Planning 30 : 890-898 (1997) .
8. Lee Y. G., "The influence of security and risk perception on the reuse of internet banking", The Journal of MIS Research, Vol.17, No.1, 2007, pp.77-93

24

References

contd.....

Websites

1. www.cryptography.com
2. www.quantenkryptographie.at
3. www.physorg.com
4. www.research.ibm.com/journal
5. www.itsoc.org
6. www.wiziq.com
7. www.wikipedia.org
8. www.google.com

Books

1. Cryptography and Network Security By William Stalling.
2. Quantum Communications and Cryptography By Alexander V. Sergienko.
3. Quantum Cryptography and Secret-Key Distillation By Gilles Van Assche.
4. E- Commerce Strategies, Technology & applications By David

25

Thank-You

26